In the Claims

No Claims are currently amended.

Claims 4-5, 14-15, 21-22, 26, and 29 were previously canceled.

Claims 1-3, 6-13, 16-20, 23-25, 27-28, and 30-33 are pending and are listed below.

1. (Previously Presented) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature at a server computing device;

receiving a security patch at the server computing device;

identifying, from the server computing device, a vulnerable binary file located on a client computing device based on the binary signature, the client computing device being remote from the server computing device; and

updating, from the server computing device, the vulnerable binary file located on the client computing device with the security patch.

2. (Previously Presented) A processor-readable medium as recited in claim 1, wherein the identifying a vulnerable binary file located on a client computing device includes comparing a bit pattern of the binary signature against binary files located on the client computing device, the bit pattern associated with a security vulnerability.

3. (Previously Presented) A processor-readable medium as recited in claim 1, wherein the updating the vulnerable binary file located on the client

computing device includes installing the security patch on the client computing device from the server computing device.

4. (Canceled)

5. (Canceled)

6. (Previously Presented) A processor-readable medium as recited in claim 1, wherein the receiving includes receiving the binary signature and the security patch from a distribution server configured to distribute to the client computing device, binary signatures that identify vulnerable files and security patches configured to fix the vulnerable files.

7. (Original) A server comprising the processor-readable medium as recited in claim 1.

8. (Previously Presented) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature that identifies a security vulnerability in a binary file;

receiving a security patch configured to fix the security vulnerability in the binary file; and

distributing the binary signature and the security patch to a plurality of servers.

9. (Original) A processor-readable medium as recited in claim 8, wherein the distributing includes:

sending a notice to each of the plurality of servers regarding the security vulnerability and the available patch;

receiving a request to send the binary signature and the security patch; and

sending the binary signature and the security patch in response to the request.

10. (Original) A distribution server comprising the processor-readable medium as recited in claim 8.

11. (Previously Presented) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature from a server;

searching for the binary signature in binary files located on a client computer;

sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature;

receiving the security patch from the server; and

updating on the client computer the binary file with the security patch.

12. (Original) A client computer comprising the processor-readable medium as recited in claim 11.

13. (Previously Presented) A method comprising:

receiving a binary signature from a server and at a client computer;

searching on the client computer for a vulnerable file based on the binary signature;

if a vulnerable file is found on the client computer, requesting a security patch from the server;

receiving the security patch from the server and at the client computer in response to the request for the security patch from the client computer; and

fixing the vulnerable file with the security patch received from the server.

14. (Canceled)

15. (Canceled)

16. (Previously Presented) A method as recited in claim 13, wherein the fixing includes installing the security patch on the client computer.

17. (Original) A method as recited in claim 13, wherein the searching includes comparing the binary signature to binary information on a storage medium of the client computer.

18. (Previously Presented) A method as recited in claim 17, wherein the binary information is selected from a group comprising:

an operating system;

an application program file; and

a data file.

19. (Previously Presented) A method as recited in claim 17, wherein the storage medium is selected from a group comprising:

a hard disk;

a magnetic floppy disk;

an optical disk;

a flash memory card;

an electrically erasable programmable read-only memory; and

network-attached storage.

20. (Previously Presented) A method comprising:

receiving, at a scan/patch server, a binary signature and a security patch from a distribution server;

searching, by the scan/patch server, on a client computer for a vulnerable file associated with the binary signature; and

if a vulnerable file is found, fixing, by the scan/patch server, the vulnerable file on the client computer with the security patch.

21. (Canceled)

22. (Canceled)

23. (Previously Presented) A computer comprising:

means for receiving, at a client computer, a binary signature from a server;

means for searching for a vulnerable file located on the client computer based on the binary signature;

means for requesting, by the client computer, a security patch from the server if a vulnerable file is found on the client computer;

means for receiving the security patch from the server at the client computer responsive to the request for the security patch; and

means for fixing the vulnerable file with the security patch received from the server.

24. (Previously Presented) A server comprising:

means for receiving, at a scan/patch server, a binary signature and a security patch from a distribution server;

means for scanning, from the scan/patch server, a client computer for a vulnerable file associated with the binary signature; and

means for fixing, from the scan/patch server, the vulnerable file on the client computer with the security patch if a vulnerable file is found on the client computer.

25. (Previously Presented) A computer having a tangible component and comprising:

binary information;

a storage medium configured to retain the binary information;

a scan module configured to receive a binary signature from a server and scan the binary information on the computer for the binary signature; and

a patch module configured to request a security patch from a server and install the security patch from the server if the binary signature is found in the binary information on the computer.

26. (Canceled)

27. (Previously Presented) A computer as recited in claim 25, wherein the binary information is selected from a group comprising:

an operating system;

an application program file; and

a data file.

28. (Previously Presented) A computer having a tangible component and comprising:

binary files;

a storage medium configured to retain the binary files;

a binary signature; and

a security patch module configured to receive the binary signature from a server and to scan the binary files on the computer in search of the binary signature;

a binary file that includes the binary signature; and

a security patch;

wherein the security patch module is further configured to request the security patch from the server upon locating the binary signature within the binary

file, and to apply the security patch to the binary file that includes the binary signature.

29. (Canceled)

30. (Previously Presented) A distribution server having a tangible component and comprising:

a database; and

a distribution module configured to receive a binary signature and a security patch, store the binary signature and the security patch in the database, and distribute the binary signature and the security patch to a plurality of servers.

31. (Original) A distribution server as recited in claim 30, wherein the distribution module is further configured to receive a request from a server for the binary signature and the security patch and to distribute the binary signature and the security patch to the server in response to the request.

32. (Previously Presented) A server having a tangible component and comprising:

a binary signature associated with a security vulnerability in a binary file;

a security patch configured to fix the security vulnerability in the binary file;

a database embodied as a storage medium and configured to store the binary signature and the security patch;

a scan module configured to scan, from the server, binary files on a client computer for the binary signature and to update, from the server, the binary file on the client computer with the security patch if the binary signature is found, wherein the client computer is remote from the server.

33. (Previously Presented) A server as recited in claim 32, wherein the scan module is further configured to receive the binary signature and the security patch from a distribution server and to store the binary signature and the security patch in the database.